

# SORBA la Interacción de TLS y SRTP-RTP en el CUBO usando IOS CA

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración del CUBO](#)

[Configuración CUCM](#)

[Verificación](#)

[Troubleshooting](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

## Introducción

Este documento describe los fundamentos del Session Initiation Protocol (SIP) Transport Layer Security (TLS) y del protocolo Real-Time Transport seguro (SRTP) sobre el Cisco Unified Border Element (CUBO) con un ejemplo de configuración.

La comunicación por voz segura sobre el CUBO se puede dividir en dos porciones:

- Asegure la señalización – Aplicaciones TLS del CUBO de asegurar la señalización sobre el SORBO y la seguridad de protocolos en Internet (IPSec) para asegurar la señalización sobre H.323
- Asegure los media – SRTP

## Prerequisites

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Los archivos del administrador de las Comunicaciones unificadas de Cisco (CUCM) Certificate Trust List (Lista de confianza del certificado) (CTL) se crean para el Mezclado-MODE
- Los Teléfonos IP se registran en el modo seguro (el cifrado)
- Se hace el voip y la configuración de dial-peer básicos del servicio de voz del CUBO

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CUCM 10.5

- CUBO – 3925E con IOS 15.3(3)M3
- Cisco IP Communicator (CIPC)

## Antecedentes

- TLS - TLS y su precursor, Secure Sockets Layer (SSL), son los protocolos criptográficos que proporcionan la Seguridad de comunicación sobre Internet.

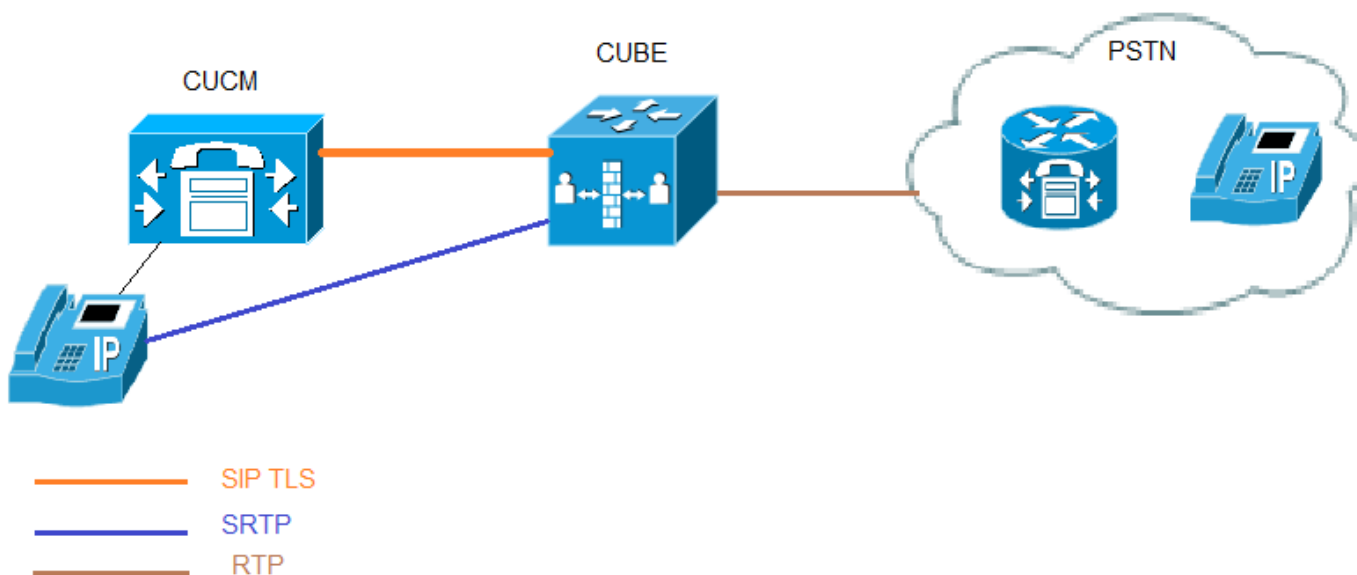
En las equivalencias del modelo del Open Systems Interconnection (OSI), TLS/SSL se inicializa en la capa 5 (la capa de sesión) y después trabaja en la capa 6 (la capa de presentación). En ambos los modelos, TLS y el SSL trabajan en nombre de la capa de transporte subyacente, cuyos segmentos llevan los datos encriptados.

- Certificate Authority (CA) - La entidad confiable esa los problemas certifica: Cisco o una entidad de tercera persona.
- Autenticación del dispositivo - Proceso que valida la identidad del dispositivo y se asegura de que la entidad es lo que demanda ser antes de que se haga una conexión.
- Cifrado - Proceso de traducir los datos en el texto cifrado que asegura la confidencialidad de la información. Solamente el receptor deseado puede leer los datos. Requiere un algoritmo de encriptación y una clave de encriptación.
- Público/clave privadas - Claves que se utilizan en el cifrado. Las claves públicas están extensamente - disponible, pero las claves privadas son sostenidos por sus propietarios respectivos. El cifrado asimétrico combina ambos tipos.

## Configurar

### Diagrama de la red

En esta imagen, el ejemplo de configuración para configurar el SORBO TLS y SRTP entre el teléfono CUCM/IP y el CUBO se muestra. Internetworks del CUBO entre el SRTP y el Real-Time Transport Protocol (RTP). El CUBO actúa como IOS CA y CUCM utilizaría los certificados autofirmados.



# Configuración del CUBO

## 1. Reloj de la configuración y servidor HTTP del permiso

Sincronice los relojes en el servidor y el trustpoints del cliente (CUBE/OGW/TGW) de CA. Si no, hay problemas con la validez de los Certificados publicados por el servidor de CA.

```
Secure-CUBE#clock set <hh:mm:ss> < Day of the month> <MONTH> <Year>
```

Or

```
Ntp server <IP Address>
```

Uso HTTP del trustpoints del cliente de recibir el certificado de CA.

```
Secure-CUBE(config)#ip http server
```

## 2. Genere un par de claves RSA

Este paso genera el soldado y las claves públicas.

En este ejemplo, el CUBO es apenas una escritura de la etiqueta. Puede ser cualquier cosa.

```
Secure-CUBE(config)#crypto key generate rsa general-keys label CUBE modulus 1024
```

The name for the keys will be: CUBE

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 0 seconds)

```
Secure-CUBE(config)#
```

## 3. Servidor IOS CA de la configuración

En este ejemplo, el servidor de CA se nombra cubo-Ca.

```
crypto pki server cube-ca
```

```
database level complete
```

```
no database archive
```

```
grant auto
```

```
lifetime certificate 1800
```

```
Secure-CUBE(cs-server)#no shut
```

%Some server settings cannot be changed after CA certificate generation.

% Please enter a passphrase to protect the private key

% or type Return to exit

Password:

Re-enter password:

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 0 seconds)

% Certificate Server enabled.

```
Secure-CUBE(cs-server)#
```

## 4. Cree el trustpoints PKI para el cubo para la comunicación de TLS.

En este ejemplo, el nombre del trustpoint para el CUBO es CUBE-TLS. La dirección IP usada en el URL de la inscripción debe ser interfaz local en el CUBO. El asunto usado en este paso debe hacer juego en el asunto X.509 en el perfil de seguridad del trunk del SORBO CUCM. La mejor práctica es utilizar el hostname con el Domain Name (si se habilita el Domain Name).

Par clave del socio RSA creado en el paso 2.

```
crypto pki trustpoint CUBE-TLS
enrollment url http://X.X.X.X:80
serial-number none
fqdn none
ip-address none
subject-name CN=Secure-CUBE
revocation-check none
rsakeypair CUBE
```

5. Autentique el trustpoint con el servidor de CA y valide el certificado de CA.

```
Secure-CUBE(config)#crypto pki authenticate CUBE-TLS
```

Certificate has the following attributes:

```
Fingerprint MD5: BCEBB5A1 1AC882F7 24BE476D 06537711
Fingerprint SHA1: CE2FEEA5 42515B33 3EF6A8F6 7E31D6DF 8E32BEB6
```

```
% Do you accept this certificate? [yes/no]: yes
```

```
Trustpoint CA certificate accepted.
```

```
Secure-CUBE(config)#
```

**6.** Aliste el trustpoint con el servidor de CA.

En este paso el CUBO recibe un certificado firmado de CA.

```
Secure-CUBE(config)#crypto pki enroll CUBE-TLS
```

```
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
```

```
Password:
```

```
Re-enter password:
```

```
% The subject name in the certificate will include: CN=Secure-CUBE
% The fully-qualified domain name will not be included in the certificate
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CUBE-TLS' command will show the fingerprint.
```

```
Secure-CUBE(config)#
```

**7.** Cree el trustpoint para el CUCM.

Si el grupo de CallManager tiene los servidores CM múltiples, después el trustpoint necesita ser creado para todos los servidores, si no la Conmutación por falla no trabaja.

```
crypto pki trustpoint cucmpub
enrollment terminal
revocation-check none
```

```
crypto pki trustpoint cucmsub
enrollment terminal
revocation-check none
```

**8.** Aliste el certificado CUCM PARA CUBICAR.

Paso 1. Login a CUCM OS admin.

Paso 2. Navegue al **Certificate Management (Administración de certificados) > al hallazgo de la Seguridad.**

### Certificate List

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR

#### Status

26 records found

#### Certificate List (1 - 26 of 26)

Rows per Page 50

Find Certificate List where Certificate begins with Find Clear Filter

Certificate	Common Name	Type	Distribution	Issued By	Ex
CallManager <a href="#">cmpub</a>		Self-signed	cmpub	cmpub	02/
CallManager-trust <a href="#">Cisco_Root_CA_2048</a>		Self-signed	Cisco_Root_CA_2048	Cisco_Root_CA_2048	05/
CallManager-trust <a href="#">Cisco_Root_CA_M2</a>		Self-signed	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/
CallManager-trust <a href="#">cmsub</a>		Self-signed	cmsub	cmsub	02/
CallManager-trust <a href="#">CAP-RTP-001</a>		Self-signed	CAP-RTP-001	CAP-RTP-001	02/
CallManager-trust <a href="#">Cisco_Manufacturing_CA</a>		CA-signed	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/
CallManager-trust <a href="#">CAPF-9a08b5fe</a>		Self-signed	CAPF-9a08b5fe	CAPF-9a08b5fe	02/

Paso 3. Haga clic el certificado del **CallManager**, después descargue y salve el archivo del .PEM tal y como se muestra en de esta imagen.

### Certificate Details for cmpub, CallManager

Regenerate
 Generate CSR
 Download .PEM File
 Download .DER File

**Status**

Status: Ready

**Certificate Settings**

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

**Certificate File Data**

```
[
Version: V3
Serial Number: 6AA0AECEC947BDCAFCC722310EE83224
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=bangalore, ST=karnataka, CN=cmpub, OU=tac, O=cisco, C=IN
Validity From: Sat Feb 07 22:39:22 IST 2015
To: Thu Feb 06 22:39:21 IST 2020
Subject Name: L=bangalore, ST=karnataka, CN=cmpub, OU=tac, O=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100d2191a26d52904ae14c3b6eb1a27607d5ca4d85251037db19141e76906d2cfcf5dca3
097fff569b7c19b9705de7624ca441617d49e08ee21a5d5cb8f3583a1f6089278b971833b6132dd4c77e
5e81866f2f4386bc16252658e5bf0c37cb844df8a53a7dc034dff225fe7127b0fba88ab96617d01c3026f1
04eea12492a8572250203010001
Extensions: 3 present
]
```

Paso 4. Abra el archivo en la libreta y copie el contenido del COMIENZAN EL CERTIFICADO PARA TERMINAR EL CERTIFICADO .

Paso 5. Pegue este certificado en el CUBO como se muestra.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
```

```
MIICojCCAagugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEWJtJTJEOMAWGA1UEChMFY2lzy28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2lwdWIxejAQBgNVBAGTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyM1oXDTEwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWVnc2NvMQwwCgYDVQQLEwN0YWMxZjAQBgNVBAMTBWNTcHVh
MRIwEAYDVQQQIEwlrYXJlYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN
aQbS289dyjCX /Vpt8GblwXediTKRBYX1J4I7iG1l1cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8ueTfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAUwUHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0
```



MIICo jCCAgugAwIBAgIQaaqCuzslHvcr8xyIx DugyJDANBgkqhkiG9w0BAQUFADBjMQswCQYDVQGEWJTTjEOMAwGAlUEChMFY2lZy28xDDAKBgNVBAsTA3RhYzEOMAwGAlUEAxMFY2lwdWIxexjAQBgNVBAGTCWthcm5hdGFrYTESMBAGAlUEBxMJYmFuZ2Fs b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGAlUEBhMCSU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLewN0YWMxDjAMBgNVBAMTBWntcHViMRIwEAYDVQQIEwlrYXRha2ExEjAQBgNVBAGTCWJhbmdhbG9yZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG1lcuPNYOh9giSeLlxgzt hMt1Md+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDA m8QTuoSSqFciUCAwEAAAAXMFUwCwYDVR0PBAQDAgK8MCCGAlUdJQQgMB4GCCsGAQUFBwMB BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0 BconMAOGCSqGSIB3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZ1/zVuXPDOn wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV RKvt461TvA5r9HGxO+KaI8v7BaWeeROBftBoRpkvqRjFt6eIHEtn7+uUIcumDASp SkX08/Ar

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

u omita el trustpoint puede ser configurado para toda la señalización del SORBO del CUBO.

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

MIICo jCCAgugAwIBAgIQaaqCuzslHvcr8xyIx DugyJDANBgkqhkiG9w0BAQUFADBjMQswCQYDVQGEWJTTjEOMAwGAlUEChMFY2lZy28xDDAKBgNVBAsTA3RhYzEOMAwGAlUEAxMFY2lwdWIxexjAQBgNVBAGTCWthcm5hdGFrYTESMBAGAlUEBxMJYmFuZ2Fs b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGAlUEBhMCSU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLewN0YWMxDjAMBgNVBAMTBWntcHViMRIwEAYDVQQIEwlrYXRha2ExEjAQBgNVBAGTCWJhbmdhbG9yZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG1lcuPNYOh9giSeLlxgzt hMt1Md+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDA m8QTuoSSqFciUCAwEAAAAXMFUwCwYDVR0PBAQDAgK8MCCGAlUdJQQgMB4GCCsGAQUFBwMB BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0 BconMAOGCSqGSIB3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZ1/zVuXPDOn wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV RKvt461TvA5r9HGxO+KaI8v7BaWeeROBftBoRpkvqRjFt6eIHEtn7+uUIcumDASp SkX08/Ar

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#





-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

Si el IOS está debajo de 15.2.2T, después transcoder del sccp de la configuración.

El transcoder del Skinny Call Control Protocol (SCCP) necesitaría el trustpoint para señalar sin embargo si utilizan al mismo router para recibir el transcoder entonces que el mismo trustpoint (CUBE-TLS) se puede utilizar para el CUBO así como el transcoder.

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIICoJCCAagugAwIBAgIQaqCuzslHvcr8xyIxuDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJlTjEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2l2dWIxExEjAQBGNVBAgTCWthcm5hdGFrYTESMBAGAlUEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0XDTE1MDIwNzE3MDkyMVowYzELMAkGA1UEBhMC
SU4xdjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBGNVBAMTBWNtcHVl
MRIwEAYDVQQQIEwlrYXJlYXRha2ExEjAQBGNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKCGYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS289dyjCX//Vpt8GblwXediTKRBYX1J4I7iG11cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQgqMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBAQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/lZfv
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicuDASp
SkXO8/Ar
```

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

## Configuración CUCM

### 1. Certificado IOS del CUBO de la exportación a CUCM.

Paso 1. Certificado IOS de la exportación. Copie el certificado de CA uno mismo-firmado y sávelo como archivo del .PEM por ejemplo, Secure-CUBE.pem

Secure-CUBE(config)#**crypto pki export CUBE-TLS pem terminal**

% CA certificate:

-----BEGIN CERTIFICATE-----

```
MIIB/TCCAawagAwIBAgIBATANBgkqhkiG9w0BAQQFADASMRawDgYDVQQDEwdjdWJl
LWNhbmB4XDTE1MDIwNzE3MDkyMl0XDTE1MDIwNzE3MDkyMVowYzELMAkGA1UEAxMH
LWNhbmB4XDTE1MDIwNzE3MDkyMl0XDTE1MDIwNzE3MDkyMVowYzELMAkGA1UEAxMH
```

```
Y3ViZS1jYTCBnzANBqkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAtn3gRiUQ409jECyo
xVZzrpBRqj/HOqkVu3iRYp2C2PGRr0lVbZvb6IZIh+m4K0Du7gBASUFDAOeidJIF
TCI3+MjUN3grnvlMH32lJ5tVzAPHj9z7GdD42+gZSoHqOMlFB8z4+VDPzpoXpswI
3TFQHCFNbadF16P5VEFWv+0tHD8CAwEAAAnjMGEwDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAUnqzVazK/7qXzhkoTiAEFCvsN8rww
HQYDVR0OBBYEFJ6s72syv+6l84ZKE4gBBQr7DfK8MA0GCSqGSIb3DQEBAUAA4GB
AEfnNrB4nls8lvz0cqlpuTjID+KVyKRwYNP04zJYWCv7P+m1bpMfC/ql14z5/RzL
e5Bq6NUnxWByLR4gcFjmdS1E6NqoNX9S5ryS3xQRkXr0MiXnVngSKELUn22JUw/q
CEnHng0AvctrV/EBB2XlzYUxG0keiT8K+jv/g7+rmkF5
-----END CERTIFICATE-----
```

% General Purpose Certificate:

-----BEGIN CERTIFICATE-----

```
MIIB7TCCAaVagAwIBAgIBAgIBANBqkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIxMTEzMDI1MFoXDTE4MDIxMDEyNTYyMVowFjEUMBIGAlUEAxML
U2VjdXJlLUNVQkUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5C2JnKwtfO
F9bBVYhVwQK8y2c5NMkJCy//pisg+oforvxalPKAXj/jqDkqtDTc3NAMf2A1rk25
f50aaBrNJmq4rfJB1wLyD2a/CzybJg+QB5sVCCHTwk5jF9+YGIMVsivbrf4m+Lqi
OkZ5qxsMa5fEc/fejUsAE8yn4/mmgld/AgMBAAGjTzBNMASGA1UdDwQEAwIFoDAf
BgNVHSMEGDAwBSer09rMr/upfOGSh0IAQUK+w3yvDAdBgNVHQ4EFgQUsvUGSpaH
+XIOWVf50imcCHV8HjAwDQYJKoZIhvcNAQEFBQADgYEAYmRHLHxTgIogZYPScPmj
h69GLxXxAOTHhOsEbm/vfqk2vbYiHU09AtDDI+kNecSuOGmd7fokJMP9K1xc1i2a
vrr2qwQYqRAh68BwTjWzR3mFAGbDZzWiywv1jJ92ra3EMAUC0sJZSLzGY0+BjO/E
dEW6JUIOx3NxP2SBN1NMAQ0=
```

-----END CERTIFICATE-----

Secure-CUBE(config)#

Paso 2. Certificado de CA IOS de la carga en CUCM como CallManager-confianza.

Paso 3. Navegue al **Certificate Management (Administración de certificados)** del **> Security (Seguridad) de la administración CM OS > al certificado/a la Cadena de certificados de la carga**

Paso 4. Archivo del .PEM de la carga tal y como se muestra en de esta imagen.

**Upload Certificate/Certificate chain**

Upload Close

**Status**

**i** Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose\* CallManager-trust

Description(friendly name)

Upload File Browse... Secure-CUBE.pem

Upload Close

**i** \*- indicates required item.

2. Cree el nuevo perfil de seguridad del trunk del SORBO

Paso 1. En la administración CM navegue al > **Security (Seguridad) del sistema** > **a los perfiles de seguridad** > **al archivo del trunk del SORBO**.

Paso 2. Copie la existencia **perfil no seguro del trunk del SORBO** para crear el nuevo perfil seguro tal y como se muestra en de esta imagen.

## SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

### SIP Trunk Security Profile Information

Name*	Secure SIP Trunk Profile
Description	Secure SIP Trunk Profile authenticated by null String
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	Secure-CUBE
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input checked="" type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

### 3. Cree el trunk del SORBO al CUBO

Paso 1. Habilite el SRTP en el trunk del SORBO tal y como se muestra en de esta imagen.

## Trunk Configuration

Save Delete Reset Add New

Packet Capture Mode*	None
Packet Capture Duration	0
<input type="checkbox"/> Media Termination Point Required	
<input checked="" type="checkbox"/> Retry Video Call as Audio	
<input type="checkbox"/> Path Replacement Support	
<input type="checkbox"/> Transmit UTF-8 for Calling Party Name	
<input type="checkbox"/> Transmit UTF-8 Names in QSIG APDU	
<input type="checkbox"/> Unattended Port	
<input checked="" type="checkbox"/> SRTP Allowed	When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do
Consider Traffic on This Trunk Secure*	When using both sRTP and TLS
Route Class Signaling Enabled*	Default
Use Trusted Relay Point*	Default
<input checked="" type="checkbox"/> PSTN Access	
<input checked="" type="checkbox"/> Run On All Active Unified CM Nodes	

Paso 2. Configure el puerto destino 5061 (TLS) y aplique nuevo aseguran el perfil de seguridad del trunk del SORBO en el trunk del SORBO tal y como se muestra en de esta imagen.

**Trunk Configuration** Rel

Save Delete Reset Add New

---

**SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.95.155		5061

MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile\* Standard SIP Profile [View Details](#)

DTMF Signaling Method\* No Preference

## Verificación

```
Secure-CUBE#show sip-ua connections tcp tls detail
```

```
Total active connections : 2
```

```
No. of send failures : 0
```

```
No. of remote closures : 13
```

```
No. of conn. failures : 0
```

```
No. of inactive conn. ageouts : 0
```

```
TLS client handshake failures : 0
```

```
TLS server handshake failures : 0
```

```
-----Printing Detailed Connection Report-----
```

```
Note:
```

```
** Tuples with no matching socket entry
```

```
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'  
to overcome this error condition
```

```
++ Tuples with mismatched address/port entry
```

```
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'  
to overcome this error condition
```

```
Remote-Agent:10.106.95.151, Connections-Count:2
```

```
Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
```

```
=====
```

```
5061 16 Established 0 10.106.95.155
```

```
57396 17 Established 0 10.106.95.155
```

```
----- SIP Transport Layer Listen Sockets -----
```

```
Conn-Id Local-Address
```

```
=====
```

```
2 [10.106.95.155]:5061
```

La salida de la descripción de la voz activa de la llamada de la demostración se captura cuando se utiliza el transcoder LTI.

```
Secure-CUBE#show call active voice brief
```

```
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```

```
1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```

También cuando una llamada cifrada SRTP se hace entre el Cisco IP Phone y CUBO o gateway, un icono del bloqueo se visualiza en el teléfono del IP.

## Troubleshooting

Estos debugs son útiles para resolver problemas los problemas PKI/TLS/SIP/SRTP.

```
Secure-CUBE#show call active voice brief
```

```
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```

```
1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```